system that can use the security system of installed computer systems based on access control lists.

SUMMARY OF THE INVENTION

A method and system for registration, authorization, and control of access rights in a computer system are disclosed in the present invention. The inventive method for controlling access rights of subjects on objects in a computer system uses parameterized role types that can be instantiated into role instances equivalent to roles as known from the prior art. The required parameters are provided by the subject of the computer system. The computer system may derive the parameters from the job position of a subject or its membership in an organization unit. Furthermore, the inventive method provides relative resource sets which are instantiated into concrete resource sets and individual resources by using the same parameter values as for instantiating of role types.

The inventive system for authorization and control of access rights as disclosed in the present invention comprises capability lists providing the access rights of the subjects on the objects of a computer system on a per-subject basis. Furthermore, the inventive system comprises means for deriving access control lists from the capability lists, wherein the system provides said access rights of the subjects on the respective objects on a per-object basis. Within the inventive method, subjects are all possible types of holders of access rights within said computer system as for example persons, job positions, role instances, users, and transactions. Furthermore, objects are all possible types of resources on which access rights can be defined within the computer system as for example files, disks, displays, printers, scanners, and transactions.

The invention eliminates the disadvantages previously described for the prior art. A method for controlling access rights providing role types that can be instantiated into role instances offers the possibility to design a security system for a computer system with very high flexibility. Since only a small number of role types has to be defined it is advantageous that less computing resources have to be provided for the security system within the computer system. Furthermore, it is advantageous that less administration activities caused by the definition of only a small number of role types requires less efforts, and thus restricts the possibility and probability of errors and confusion and therefore provides a higher system security. Furthermore, it is advantageous that by providing the appropriate parameter values, the role instances of a role type can be restricted in such a way that the "Least Privilege Principle" is satisfied. Furthermore, it is advantageous that the automated generation of role instances by instantiating role types offers higher security of the computer system and higher integrity of the data within the computer system.

A role type combines a set of functional tasks with a common generic set of competencies. A role type can be viewed as a template for defining the types of access rights, objects, and transactions necessary to carry out a set of functional tasks.

A role instance, on the other hand, defines the set of concrete and specific competencies bound to a role type in a specific organization unit of the enterprise. An organization unit may be division, a department, a program, a project, a work-flow process or a combination thereof.

In one embodiment of the invention the role type is parameterized and the role instance is generated by using at least one parameter value. The use of a parameterized role type allows more flexibility of the security system and less administration activities. Furthermore, it is advantageous that the use of parameterized role types requires less computing resources for the security system.

In a further embodiment of the invention the objects of the computer systems form groups of concrete resource sets. Forming of such concrete resource sets is advantageous since it allows one to address functional groups of resources or objects with less computing efforts of the security system and less administrative overhead.

In a further embodiment of the invention the method allows the automated derivation of the concrete resource sets from parameterized relative resource sets. This offers a higher flexibility of the security system with less administration efforts. Furthermore, it is advantageous that less computing resources are required for the security system.

In a further embodiment of the invention the method provides the parameter value for instantiating the parameterized role types or the parameterized relative resource sets by the subjects of the computer system. This is advantageous since the derivation of role instances from role types or the derivation of concrete resource sets from relative resource sets can be fully automated and requires no administration efforts. This restricts the possibility and probability of errors and confusion and therefore provides a higher system security.

In a further embodiment of the invention the parameter value is provided by the job position or by the organization unit. This is advantageous since it provides a very flexible security system that requires very little administration activity when a person as a user of the computer systems changes job position or even organization unit. This requires less efforts, and thus restricts the possibility and probability of errors and confusion and therefore provides a higher system security.

In a further embodiment of the invention the job position is combined with at least one role type. This is advantageous since it allows the deriving of role instances associated with this role type by providing all necessary parameters for instantiating a role type with this job position. This allows automated derivation of role instances with no administration activity and therefore requires less efforts, and thus restricts the possibility and probability of errors and confusion and therefore provides a higher system security.

In a further step of the invention **8** the parameterized relative resource sets are associated with the role types. This is advantageous since it allows automated derivation of the concrete resource sets and objects by the same parameters as provided for the role types. This allows automated derivation of the concrete resource sets with no administration activities and therefore requires less efforts, and thus restricts the possibility and probability of errors and confusion and therefore provides a higher system security.

In a further step of the invention the inventive method performs a configuring step for deriving the role instances and the concrete resource sets and objects. This automated configuring step is performed with each administration action and provides at any time the actual and valid role instances and concrete resource sets and objects. This is advantageous since it guarantees the efficiency of the security system and guarantees the security and integrity of data within the computer system.

In a further embodiment the method specifies capability list types associated with the role types and performs an automated configuring step for deriving capability lists associated with role instances. The capability lists are instan-